Cribl

Migrate Agents with Cribl Edge

HOW-TO GUIDE

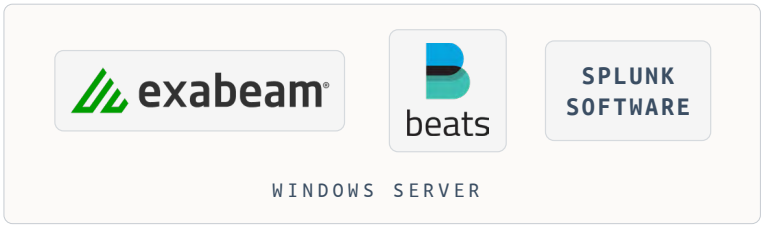
CONTENTS

The problem: legacy agents are holding you back

Let's be real—replacing agents isn't anyone's idea of a good time. But sticking with outdated, vendor-specific agents is even worse. Most were built for a simpler era, and now struggle to keep up with sprawling, modern enterprise environments.

Painful deployment, manual configurations, and tight vendor lock-in make it hard to scale or evolve your architecture. Worse yet, as your tooling evolves (and it inevitably will), you may find yourself ripping and replacing your agent again or adding yet another one. Cribl Edge eliminates this cycle by offering a single, vendor-agnostic solution that adapts to your architecture.

Customers often have at least 3-5 different agents across thousands of servers



***Multiple agents on the same endpoint**, often owned by multiple teams*

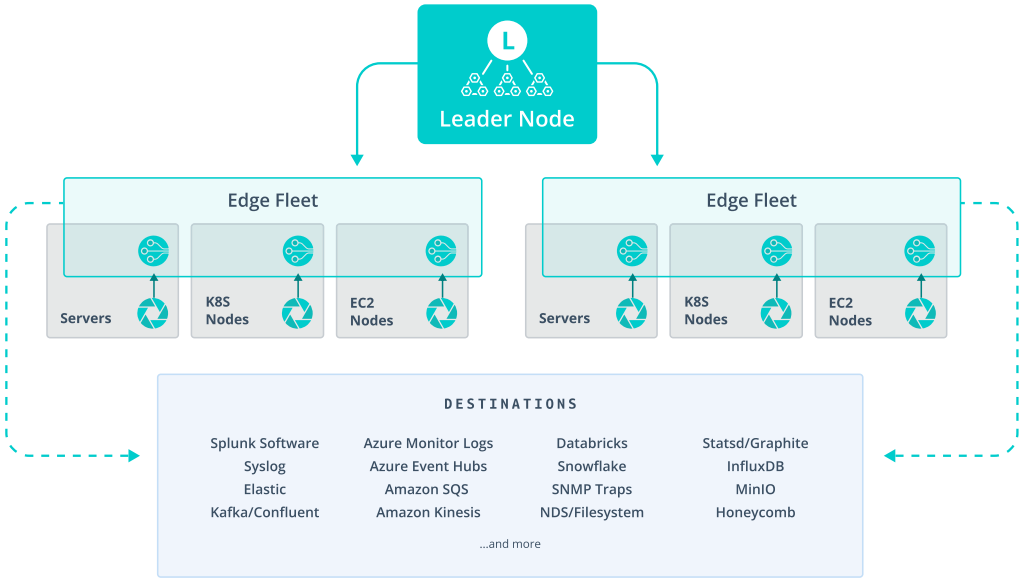
or

*Most commonly, **different tools used for varying parts of their environment**, each requiring separate management/upgrades and an SME*

Why solve it now

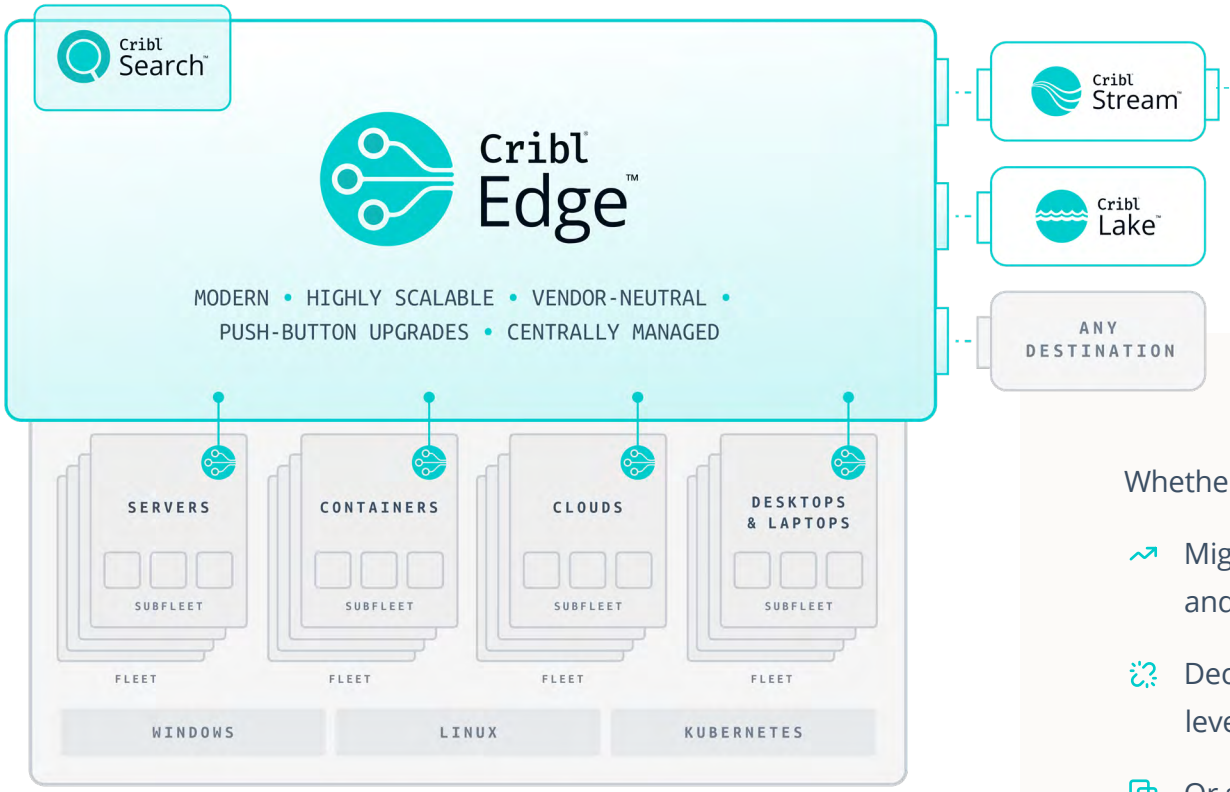
Today's environments demand a new approach. You need:

- **A modern, flexible agent** that scales across thousands of endpoints without unnecessary overhead.
- **Centralized management** to deploy, configure, and monitor at scale—without requiring access to each endpoint.
- **Push-button upgrades** to stay secure with minimal downtime.
- **Built-in troubleshooting tools** for easy investigation and comprehensive visibility.
- **Advanced data processing at the edge** to shape and filter data before it's ingested—so you don't pay more than you need to.
- **A vendor-agnostic foundation** to break free from tool sprawl and eliminate future agent migrations or additions.



In short, you need full control over your data collection, without being boxed in by your tooling.

How to solve it: Cribl Edge for streamlined migration



Whether you're:

- Migrating away from a vendor like Splunk software and its Universal Forwarder,
- Decoupling data collection from analysis to gain leverage in renewals,
- Or streamline operations by consolidating your myriad legacy agents...

Cribl Edge is easy to deploy and manage to simplify your agent migration, while giving you more flexible data collection than ever before.

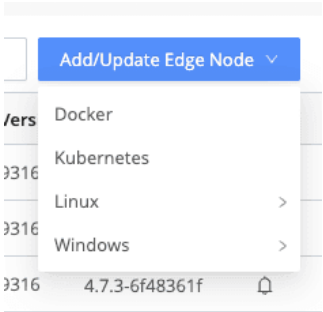
Cribl Edge: a flexible agent with unmatched ease of use

How to use Cribl Edge to simplify agent migration:

1 | Fast, mass deployment

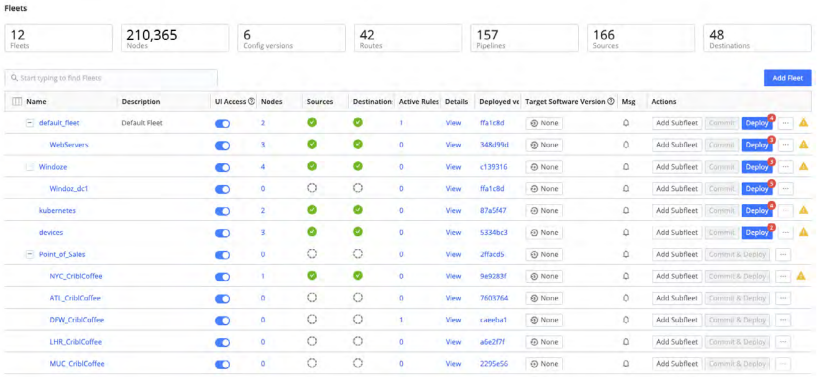
Cribl Edge offers teams the ability to rapidly deploy fleets of agents at scale. We have an intuitive UI that guides you to easily install agents in minutes, or even hundreds of agents with a simple script to put into your tool of choice such as Ansible, Terraform, Puppet, and more. Once it's installed, you no longer need to wait on host access or permission from other teams to configure and upgrade, giving your team complete control.

Because Cribl Edge is vendor-neutral, you can consolidate multiple data collection agents into a single unified data collection system. This not only reduces operational overhead but ensures consistency and efficiency across telemetry sources.



2 | Centrally configure at scale

After you deploy your agents, efficiently configuring them is simple with Cribl Edge's centralized fleet management, which lets you standardize configurations across groups of agents through your choice of hierarchical model—tailored to your organizational structure, geography, operating systems, or unique requirements. Admins can efficiently make changes across specific fleets and subfleets, and maintain version



Centrally configure at scale

Cribl Edge: a flexible agent with unmatched ease of use *(continued)*

consistency without the risk of drift and of course, all changes are tracked for auditing purposes.

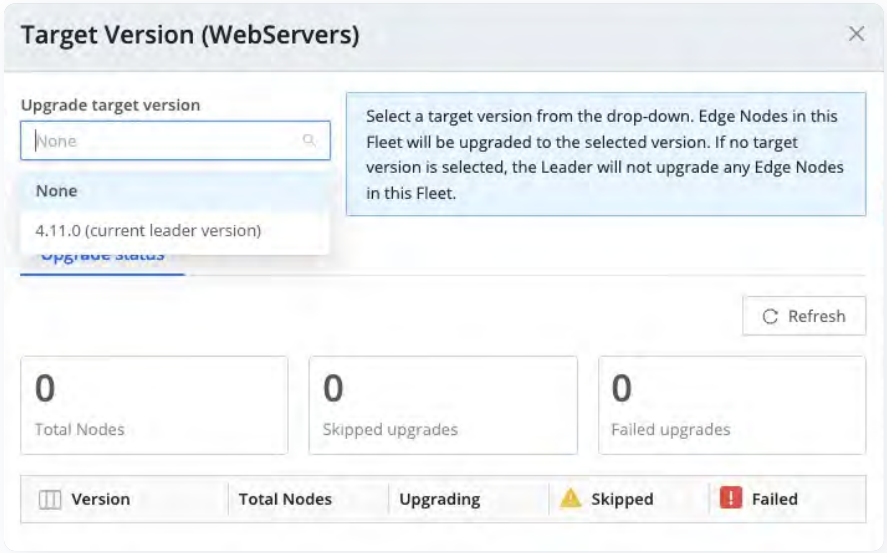
Out-of-the-box integrations with your array of tools make it easy to onboard new data sources or switch destinations. And with a UI-based pipeline builder, teams can effortlessly filter, shape, and logically route data directly at the edge.

When incidents or investigations arise, you can collect extra files within minutes directly from the user interface—no manual restarts required.

3 | Push-button remote upgrades

Cribl Edge minimizes downtime by supporting fleet-wide upgrades with no need to restart endpoints or destinations. Upgrades can be initiated remotely and directly by your team—no need to coordinate with endpoint owners. This reduces downtime and enhances your security posture.

Admins can control versioning across environments, executing upgrades when they fit operational timelines. Cribl Edge ensures agent maintenance is fully in your control.

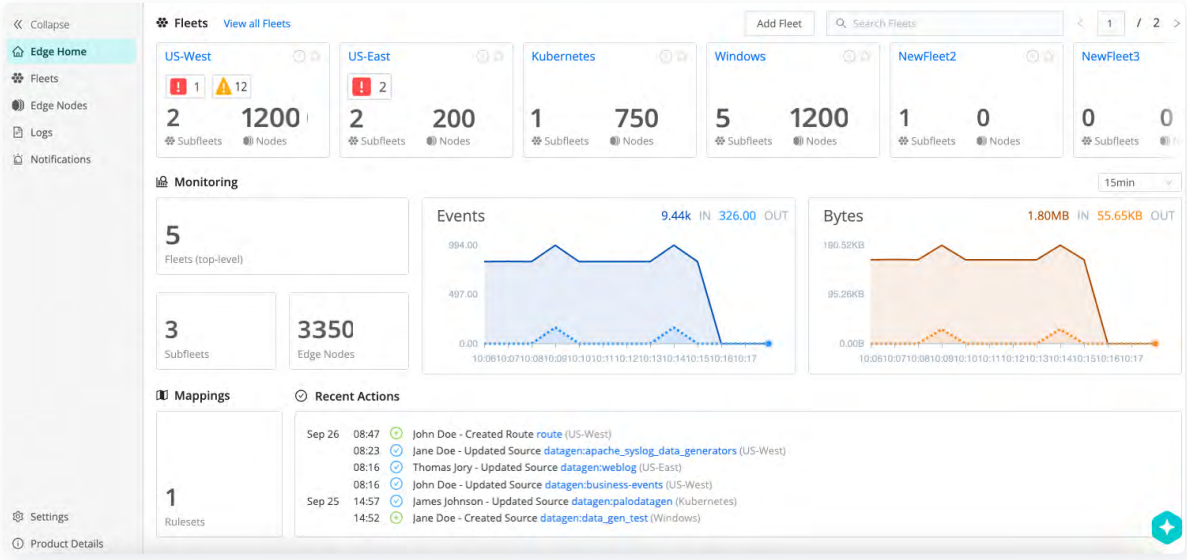


Push-button remote upgrades

Cribl Edge: a flexible agent with unmatched ease of use *(continued)*

4 | Troubleshoot with confidence

For those inevitable incidents, Cribl Edge provides comprehensive visibility across all of your Cribl Edge agents with a unified monitoring console that tracks performance, health, and connectivity. You can quickly isolate whether issues stem from the source, destination, or node.



To identify and resolve issues, you can "teleport" into individual nodes to explore metrics and logs—eliminating the guesswork from troubleshooting and dramatically reducing mean time to resolution (MTTR).

For detailed step-by-step technical guidance on deploying Cribl Edge, check out our Getting Started Guide in our Cribl Documentation.

The outcome: choice, control, and flexibility

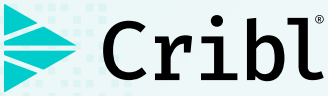
Cribl Edge gives you more than just a migration choice—it offers a long-term agent strategy built for choice, control, and flexibility. With support for routing data to your SIEM, storage, or Cribl Stream, organizations can optimize cost and performance while gaining full control over where and how telemetry is collected and processed.

Advanced edge processing lets you filter and shape telemetry data right at the source, reducing unnecessary data movement and associated license costs. With agnostic integrations and no vendor lock-in, Cribl Edge ensures your data collection remains adaptable—so you're ready for future changes in tools, keeping your organization agile and resilient.

Get Started Today

Whether you want to replace one proprietary agent or consolidate a myriad of agents across your environment, Cribl Edge makes it simple.

- **See how Cribl Edge compares** to a vendor-specific agent, such as Splunk Universal Forwarders, in this datasheet
- **Need migration help?** See this one-pager on how Cribl's Professional Services Universal Forwarder Migration offering can accelerate your move
- **Ready to consolidate your mix of legacy collection tools?** Check out our blog to learn how
- **Want to deploy right now?** Get step-by-step guidance



Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Powered by a data processing engine purpose-built for IT and Security, Cribl's product suite is a vendor-agnostic data management solution capable of collecting data from any source, processing billions of events per second, automatically routing data for optimized storage, and analyzing any data, at any time, in any location. With Cribl, IT and Security teams have the choice, control, and flexibility required to adapt to their ever-changing data needs. Cribl's offerings — Stream, Edge, Search, and Lake— are available either as discrete products or as a holistic solution.

Learn more: cribl.io | Try now: Cribl sandboxes Join us: Slack community
Follow us: LinkedIn and X (Twitter)

EB-0009-EN-1-0425